

Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

<http://people.delphiforums.com/dpj/a-one.htm>
Now available:
<http://www.atarinews.org>

Visit the Atari Advantage Forum on Delphi!
<http://forums.delphiforums.com/atari/>

==~==~==

~ NYC To Accept Bitcoin? ~ Safer Internet Day 2015 ~ Asteroids: Outpost!

- * New Agency for Cybersecurity *-
- * TurboTax Resumes E-filing Practices *-
- * Facebook To Help User Accounts After Death *-

==~==~==

->From the Editor's Keyboard
"~~~~~"

"Saying it like it is!"

Happy Friday the 13th! Well, the sentiment might be more effective had this week's issue actually made it out to the streets when it was supposed to rather than over the weekend! Sorry, I apologize for the delay this week, but I have a good excuse. Well, an excuse, whether or not you think it good or bad! The weather. That's it. More snow (and moe on the way!). I spent a good amount of time cleaning up after a few storms in preparation for the one coming this weekend. That meant "raking" the roofs, or actually climbing up to them because access to use the snow rake was limited or even impossible! A lot of time and hard work; and I'm not getting any younger!

So, I was too tired and sore to finish up the issue last night! In fact, we did some more roof-cleaning Saturday before I was able to get back to the issue. So, before I crash for the day, let's see if we can get this finished up and out to you!

Until next time...

==~==~==

Atari Coldfire - New GFA Release

Dear Ladies and Gentleman,

Mr. Pursell released a new version of GBE, which fixes many bugs and includes now all needed components for coding and compiling, so that you can start right away with building new programs for your Bees and 68k Ataris. This one is a major release!

<http://acp.atari.org>

Atari-coldfire mailing list

Atari-coldfire@lists.lnxnt.org

<https://lists.lnxnt.org/mailman/listinfo/atari-coldfire>

==~==~==

->In This Week's Gaming Section - Asteroids: Outpost, Multiplayer Survival Game
!
" BioWare's Shadow Realms Canceled!
Gamer Swatted While Live-streaming!

=~==~==

->A-ONE's Game Console Industry News - The Latest Gaming News!
"

Early Access for Asteroids: Outpost, Multiplayer Survival Game Coming Soon to PC

Atari announced the upcoming release of Asteroids: Outpost for PC. This bold re-imagining of the world-renowned 1979 arcade shooter puts players in the role of a deep space miner, as they struggle for survival in the asteroid belt. Asteroids: Outpost reinvents the classic Atari title as an open world, sandbox style, survival experience, where players mine, build and defend their base and grow their fortune as they go "from rocks to riches".

Set in the distant future, Asteroids: Outpost thrusts players into a harsh deep space environment. While on a massive, unforgiving asteroid, players face the challenges of exploring the asteroid, collecting resources, scavenging for ore, crafting equipment, and expanding their territory as they build highly customized bases - all while forming alliances and fighting off other players in challenging multiplayer gameplay. Recurring showers of smaller asteroids represent a source of wealth and a threat as players shoot down these incoming projectiles to defend their claims and harvest their components.

"Asteroids is one of the most iconic titles in Atari's portfolio of more than 200 games and franchises, and we're looking forward to ushering the game into today's digital gaming era," said Fred Chesnais, Chief Executive Officer, Atari. "We're paying homage to the original Asteroids by incorporating classic features such as asteroid blasting capabilities, while introducing a completely new premise and gameplay. Asteroids: Outpost will appeal to both fans of the classic Asteroids as well as enthusiasts of immersive survival games and expansive MMOs."

Developed by Salty Games, Asteroids: Outpost will be available on PC. To keep up with the latest on Asteroids: Outpost, visit www.asteroidsoutpost.com. Fans can also join the conversation by liking Asteroids: Outpost on Facebook at <https://www.facebook.com/asteroidsgame> and following Asteroids: Outpost on Twitter, @Atari_Asteroids.

BioWare's Multiplayer PC Game Shadow Realms Canceled

Following the publication of this story, BioWare Austin officially announced the cancellation of Shadow Realms. The developer will now focus its efforts on other projects, but mostly PC MMO Star Wars: The Old Republic, BioWare Austin general manager Jeff Hickman explains in a statement posted on the game's website. You can read his full statement below.

"Today I'm sharing some important news about Shadow Realms and our BioWare Austin studio.

We've made the decision to not move forward with development of Shadow Realms. We fully recognize that this news is disappointing to some of our fans, so I want to explain more behind this decision.

While the team did amazing work on the game concept and we got lots of great feedback from our fans at events and through other game testing, right now there are other projects for the team to work on within the BioWare studios for the coming year and beyond. We've got an incredibly talented team here at the Austin studio, and they are excited and already deep on new projects within the BioWare family, ones that will make some great BioWare games even better.

These include additional ongoing enhancements to the award-winning Dragon Age: Inquisition, as well as the next game in the Mass Effect series and other new IP.

But the biggest focus for our team in BioWare Austin will be on Star Wars: The Old Republic. As every Star Wars fan knows, this is a massive year in the Star Wars universe. We have some great plans for expanding this epic game this year, and look forward to sharing the news about those plans with our players in the coming weeks.

For all the people that registered for the Shadow Realms Closed Alpha, we're working on a way to say thank-you for signing up. To all those players that gave us feedback at Gamescom and PAX, and those that shared their thoughts and impressions in the past months, we thank you for being part of the conversation."

The original story is below.

Following a report last month that claimed BioWare's 4v1 PC online game Shadow Realms had been rebooted for Xbox One and PlayStation 4, sources told Game Informer today that the title has been canceled outright.

Multiple sources at publisher Electronic Arts said the game is no longer in the works, though it's unclear as to why the game has been shut down or if there will be layoffs as a result.

EA declined to comment when approached by Game Informer.

The game, which was announced during Gamescom less than a year ago, was in development at Star Wars: The Old Republic developer BioWare Austin.

Set in a modern fantasy world, Shadow Realms was described as an "online-only" RPG that would offer cooperative 4v1 gameplay. Four players can fight against an enemy known as the Shadowlord, or you can play as the Shadowlord.

"This game brings us back to our roots in the realm of classic Pen and

Paper RPG, but also delivers something that's completely new and innovative for our fans," Hickman said at the time. "Shadow Realms is a new BioWare RPG that has the hallmarks of all BioWare games with a rich story, a unique world setting, and deep combat progression, but built as an interactive experience that evolves the genre and broadens the appeal to online gamers all over the world."

Gamer Swatted While Live-streaming on Twitch.TV

A gamer has posted a video of his tearful reaction after he was swatted in the middle of a live Twitch stream of RuneScape.

The video shows him just moments after armed police stormed his house, pointed their guns at his 10-year-old brother who answered the door, and forced the gamer himself to lie face down on the floor in yet another swatting incident in the gamer community.

I see you posting my address. I had police point a gun at my little brothers because of you. They could have been shot. They could have died. Because you chose to swat my stream. I don't give a sh*t about what you have against me, or what I did to you. For that I am ... I am at a loss for words. Your gripe is with me. So let it be with me. But do not involve my family in any way, shape or form with this. They don't deserve that.

Joshua Peters, 27, goes by the alias Koopatropa787 to live-stream his gaming on Twitch.TV for almost 60,000 followers from his home in St. Cloud, Minnesota, in the US.

On Wednesday, while he streamed during RuneScape, his noise-canceling headphones muffled the sounds of the 10 armed police who stormed his house.

His live stream from that day shows Peters's reaction when his mother's voice penetrates the headphones to inform him that the police are there.

He arose, confused and concerned, told his followers that the police were there, and left the screen.

After some 15 minutes, Peters returned to the live stream to leave the emotional message above for whomever did this to him and his family.

The next day, he told The Guardian that he hadn't seen it coming:

My channel's not crazy big, like some of these other mainstream streamers. I just didn't expect that. I was going upstairs, and before I knew it, my face was on a tile on the ground, hands wide open and a bunch of police officers with assault rifles.

Swatting is the practice of making bogus emergency calls, as a prank or as revenge, with the hopes of getting armed law enforcement or other emergency responders to descend on a victim.

In Peters's case, he told viewers later, the perpetrator called to tell police that someone "had shot their roommate and now they were pointing their gun at them". "Two gun shots" were apparently heard before the call ended.

Swatting is far from new, particularly with regards to Twitch.TV, where it's becoming more and more common, with the responsible trolls seldom suffering consequences.

In fact, a live video platform such as Twitch adds a voyeuristic twist to this already puerile, dangerous stunt, allowing the perpetrators to watch the whole situation unfold, live, with a built-in audience.

Although this was the first swatting incident the St. Cloud police say they've experienced, like most police nowadays, they're familiar with the practice.

In fact, just the mention of Twitch helped to defuse the situation, Peters said:

When we were all laying down, I spoke out. I said 'I stream on Twitch.TV, I m being swatted, and someone probably prank-called this'. And then the tone shifted as soon as I said 'I'm streaming on Twitch.TV.'

But the swatter(s) didn't leave it at just one incident. He, or she, or they, tried again, posing as one of Peters's family members to call police and tell them he was suicidal about the raid.

Fortunately, the police didn't rise to the bait the second time. They made sure to vet the call before wasting their time responding to yet another prank.

Peters is one of many who've been either randomly targeted or purposefully singled out as part of ongoing campaigns of harassment.

A recently launched network, Crash Override is aimed at helping such victims.

The network, which its founders describe as an "online anti-harassment task force", is devoted to helping victims of doxing/swatting in the ongoing Gamergate battle.

One of the would-be swatting victims helped out by the proactive work of the network was Israel Galvez, a web developer and Gamergate critic who was the target of a swatting attempt that came out of a forum linked to Gamergate.

Crash Override, which monitors known troll forums, in January gave police a heads-up about Galvez's likelihood of being targeted.

When police subsequently received a bogus message about a "cylinder thing with duct tape wrapped around it" that was supposedly to be found within their target's house, police knew to dial down their reaction.

In other words, they knocked with their fists, not with their boots, averting a potentially dangerous incident.

Gamers, if you're live streaming, please be careful.

As Peters's horrific experience shows, these vicious attacks can come out of nowhere, sparked by absolutely nothing, rising up to silently blindside both you and the innocents around you.

=~==~==

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

U.S. To Establish New Agency for Cybersecurity

The U.S. government is creating a new agency to monitor cybersecurity threats, pooling and analyzing information on a spectrum of risks, a senior Obama administration official said on Tuesday.

The Cyber Threat Intelligence Integration Center (CTIIC) will be an intelligence center that will connect the dots between various cyber threats to the nation so that relevant departments and agencies are aware of these threats in as close to real time as possible, the official said on condition of anonymity.

Obama has moved cybersecurity to the top of his 2015 agenda after recent hacking attacks against Sony Pictures, Home Depot Inc, Anthem Inc and Target Corp and the federal government itself.

The Democratic president sees it as an area of cooperation with the Republican-led Congress.

Various federal agencies have cybersecurity components, including the National Security Agency, Department of Homeland Security, the FBI and the CIA.

The Obama administration is trying to connect the agencies so that there s one belly button for the entire U.S. government, Shawn Henry, president of CrowdStrike cybersecurity agency, said on the CBS This Morning program.

"That s a good strategy. It s important because there s so many different pieces of intelligence coming in. You ve got to collaborate and put it together," he said.

The CTIIC will aim for seamless intelligence flows among centers, including those responsible for sharing with the private sector, the official said.

The White House counterterrorism coordinator, Lisa Monaco, will announce the new center in an address on Tuesday.

The Obama administration likens the new agency to the National Counterterrorism Center established after the Sept. 11, 2001, attacks, following criticism that U.S. intelligence agencies were not communicating with each other.

It will have a similar broad focus of providing integrated, all-source analysis of threats, the official said.

"No existing agency has the responsibility for performing these

functions, so we need these gaps to be filled to help the federal government meet its responsibilities in cybersecurity," the official said.

Congress has tried for years to pass legislation to encourage companies to share data from cyberattacks with the government and each other, but efforts were stymied by liability issues and privacy concerns of citizens.

Last month, President Barack Obama proposed legislation to strike a balance, offering liability protection to companies that provide information in near real time to the government, while requiring them to strip it of personal data.

The Washington Post first reported the agency's creation.

FireEye Is "First in the Door" on Big Cyberattacks

As hackers invade the computer systems of major companies with greater frequency and their corporate victims scramble to contain the damage and prevent future intrusions, these are boom times for cybersecurity sleuths.

Perhaps no security specialist has benefited more than a small but fast-growing company called FireEye, which is based in Silicon Valley and staffed with a roster of former military and law-enforcement cyberexperts.

FireEye has been called in to investigate the high-profile cyberattacks against Target, JPMorgan Chase, Sony Pictures and, just last week, Anthem, the country's second-largest health insurer,

"In any high-profile cyber breach, FireEye is usually first in the door," said Daniel Ives, a technology industry analyst at FBR Capital Markets.

FireEye CEO David DeWalt calls his employees "cyber SEALs" as in Navy SEALs.

After a slew of prominent cases last year, FireEye ranked first in a recent Piper Jaffray survey of corporate IT officials who were asked which security contractor they planned to hire in 2015.

But Wall Street isn't totally sold. The company, which made its market debut in late 2013, has roughly doubled its sales in each of the last four years but hasn't yet turned a profit. The stock soared to nearly \$100 a year ago after FireEye bought hot security startup Mandiant. But disappointing earnings and a sell-off by early investors caused the stock to plummet last spring.

Since then, FireEye shares have limped along, trading mostly in the \$40 and below range. Analysts say the company could be ripe for takeover by a bigger tech firm, such as IBM Corp., Cisco Systems Inc. or Hewlett-Packard Co.

FireEye, based in Milpitas, Calif., gained some goodwill on Wednesday with a fourth-quarter earnings report that showed sales of \$143 million, nearly tripled from a year ago, and a smaller-than-expected loss of \$105.7

million. Its stock popped 12 percent Thursday.

"We're a growth company with a huge opportunity," DeWalt told The Associated Press. He said FireEye's strength lies in its software capabilities and its deep bench of experts trusted by government officials. As a result, when a company like Sony gets hacked, it usually calls authorities first, "and the second call is to us, or vice versa," he said.

Competitors like Palo Alto Networks Inc., CloudFlare and ProofPoint offer their own innovative approaches to cyberdefense. Rivals like CrowdStrike are known for tracking overseas hackers, while computer forensics firm Stroz Friedberg has its own lineup of ex-federal prosecutors and cops. But FireEye has become a "marquee name," said industry analyst Jon Oltsik of the Enterprise Strategy Group.

It holds that status at a time when DeWalt says there's been a "massive increase" in cyberattacks sponsored by governments. FireEye has played a role in investigations that pointed the finger at Chinese authorities seeking economic secrets, supporters of a Syrian president battling anti-government rebels, and a North Korean regime bent on disrupting the studio behind an irreverent film comedy.

A veteran tech executive, the plain-spoken DeWalt holds a top government security clearance and is a respected figure in Silicon Valley. His last job was CEO at McAfee, which Intel bought in 2010. These days, he contends software from industry leaders like McAfee is no longer effective.

While older companies sold firewalls or anti-virus programs that block known malware, FireEye founder Ashar Aziz developed a system for spotting threats that haven't been tracked before. Aziz, a former Sun Microsystems engineer, started FireEye in 2004 and is vice chairman today. His system uses software to simulate a computer network and check programs for suspicious behavior, before allowing them into the network itself.

"The world has changed. The bad guys have changed. And new solutions are needed," said Matt Trotter, a managing director at Silicon Valley Bank, who's seeing increased investment by venture capitalists in security startups.

FireEye raised its profile last year by acquiring Mandiant, known for expertise in assessing damage and tracing the source of cyberattacks. Mandiant founder Kevin Mandia, a former U.S. Air Force investigator, is now FireEye's chief operating officer. His group handles high-profile "crisis response," but their work also helps FireEye sell its other security tools.

While businesses are spending more on information security, FireEye itself has spent heavily on research, development, sales and marketing. Analysts expect it will post losses for the next two years.

"No one can deny they are a clear leader in cybersecurity, but ultimately the company has not delivered the financial results yet," said FBR's Ives. If that doesn't change over the next year, he added, "I'd view it as a top acquisition for a large company such as a Cisco or an IBM."

In her first interview since her exit as co-chairman of Sony Pictures, Amy Pascal opened up about her departure and acknowledged it wasn't voluntary.

Speaking to journalist Tina Brown at the Women in the World conference Wednesday night in San Francisco, Pascal joked, "All the women here are doing incredible things in this world. All I did was get fired."

After a long reign as the head of Sony Pictures, the studio last week announced Pascal was stepping down and would start a new production venture at Sony. In her new role as producer, she has already inherited several of the studio's biggest upcoming projects, including Sony's next Spider-man film, to be made in partnership with Marvel Studios.

"I'm 56," she said at the summit. "It's not exactly the time that you want to start all over again. But it's kind of great and I have to and it's going to be a new adventure for me."

Pascal also spoke candidly about the trauma of the hacking attack that preceded her departure. When the extent of the damage was still unraveling and personal information was found to be stolen, Pascal said "everybody was really scared."

"But nagging in the back of my mind, and I kept calling them, like, 'They don't have our emails, right? Tell me they don't have our emails.' 'No, no no,'" recalled Pascal. "Well, then they did. That was a bad moment."

Pascal came under fire, in particular, for emails with producer Scott Rudin in which the two joked about President Barack Obama's presumed taste in movies. Other emails revealed a furious Rudin calling Angelina Jolie names ("the first person I talked to was Angie after that email," said Pascal) and showed her tussling with the powerful producer ("We've been having an ongoing fight since the moment we met," she said of Rudin).

"Everyone understood because we all live in this weird thing together called Hollywood," said Pascal. "If we all actually were nice, it wouldn't work."

Brown founded the Women in the World conference five years ago to bring together women leaders to share stories and advice. Long considered the top female executive in Hollywood, Pascal was known for, among other things, supporting female filmmakers. Speaking to Brown, she said much still needed to change.

"The most important thing we can do in our business is make movies with female protagonists and movies with female villains and movies where the plot of the movie is about them," said Pascal. "The worst thing you can do is be on the sidelines."

Pascal was also entertainingly frank about the inner-workings of the movie business. She called hypersensitive actors "bottomless pits of need."

Said Pascal: "You've never seen anything like it."

Anonymous Takes Down Dozens of "Terrorist" Social Media Accounts in #OpISIS

Anonymous hacktivists, in conjunction with RedCult, have ramped up efforts to disrupt ISIS by zeroing in on social media accounts allegedly used by the terrorist group for recruitment and propaganda purposes.

Against a backdrop of increased military action by allied forces against ISIS, hackers flying the Anonymous flag have unveiled a new operation - dubbed #OpISIS - which aims to take down websites and email accounts, as well as expose Islamic militants, according to a message recently posted on PasteBin.

Greetings citizens of the world, we are Anonymous,
Operation ISIS Continues:

First we need to clarify few a things.

We Are: Muslims, Christians, Jews...

We Are hackers, crackers, Hacktivist, phishers, agents, spies, or just the guy from next door.

We Are students, administrators, workers, clerks, unemployed, rich, poor, We are young, or old, gay or straight.

We wear smart clothes or rugs, we are hedonists, ascetics, joy riders or activists.

We come from all races, countries, religions, and ethnicity.

UNITED AS ONE, DIVIDED BY ZERO...

We Are Anonymous.

-REMEMBER...THE TERRORISTS THAT ARE CALLING THEMSELVES ISLAMIC STATE, ISIS), ARE NOT MUSLIMS!!!.

In the statement and an accompanying two minute video, an Anonymous spokesperson explains how the group sees ISIS as a virus that it says it intends to cure.

Part of the treatment appears to be the takedown of Facebook and Twitter accounts. The document on PasteBin lists a total of 90 Twitter accounts which the group says it has taken offline due to their affiliation with ISIS.

It also says it's keeping twelve Facebook accounts under continuing surveillance after they were found to have been "keeping contact with the terrorists (ISIS) in Syria & Iraq".

In a similar offensive last month, Anonymous launched #OpCharlieHebdo in response to the terrorist attacks in Paris, claiming responsibility for the downing of dozens of "Jihad sites".

TurboTax Resumes E-filing Following Torrent of Fraudulent Tax Returns

Intuit, the makers of the popular TurboTax app, stopped the e-filing of all state tax returns in the US on Thursday due to a surge in fraudulent filings but then recommenced on Saturday after having taken security measures to help clean up the mess.

The filing freeze came after several states refused to accept the returns after seeing a deluge of phony filings.

Utah, the first state to reach out to Intuit, issued a statement on Thursday, saying that the state tax commission had discovered 28 fraud attempts that "originate from data compromised through a third-party commercial tax preparation software process," as well as 8,000 returns flagged as potentially fraudulent.

According to Utah's state tax commission, as of Thursday, 18 other states had identified similar problems.

Intuit said in a press release on Friday that an ongoing investigation hasn't yet turned up evidence that its own systems had leaked the stolen information that's being input into the bad returns.

Rather, preliminary findings are indicating that the identity details were squeezed from external sources.

That could be any number of sources.

Intuit said on Thursday that it was working with state agencies to address growing concern over state tax fraud, which, together with improper payments, takes a \$5 billion bite out of revenue every year, according to the Internal Revenue Service: an estimate that's growing along with the rise of cyberfraud.

As of 3 pm PST on Saturday, TurboTax was back filing state returns.

To do that, it plugged in several security measures, one of which was multifactor authentication.

Multifactor or two-factor authentication (2FA) is a good stumbling block for identity thieves.

Most online 2FA systems work by asking for your username and password, which may stay the same for weeks, months or years, and then asking you for a passcode that changes every time you login.

Your passcode might come from a dedicated security token that displays a sequence of numbers that changes every minute, or you might receive a text message on your mobile phone with the passcode in it.

To read more about the hows and whys of 2FA, check out Chet Wisniewski's recent post: The power of two - All you need to know about two-factor authentication.

Not all US states require tax returns to be filed. Intuit says that filing of federal returns wasn't affected.

The state of Minnesota was one of the states that had stopped accepting TurboTax state returns.

A spokesperson for the Department of Revenue there said that the agency had resumed accepting e-filings from TurboTax on Saturday, following Intuit's announcement that it had taken steps to combat the fraud.

The state's recommendation for worried taxpayers was don't worry about it: we'll call you if we spot a problem, spokesperson Janelle Tummel said:

If you already filed your return using TurboTax, you do not need to do anything. We will review your return and contact you if we identify

issues.

To assist customers who believe they're victims of tax fraud, Intuit has set up a dedicated toll-free number, 800-944-8596, with direct access to specially trained identity protection agents who can provide support and filing assistance.

D-Link Routers Vulnerable to DNS Hijacking

D-Link's DSL-2740R router is susceptible to traffic rerouting and DNS hijacking, according to Bulgarian security researcher Todor Denev.

Unfortunately, Denev went public with his discovery before alerting D-Link or any other potentially affected manufacturer, in what could be argued to be an irresponsible form of disclosure.

The DSL-2740R is no longer a member of D-Link's current line-up but is still supported.

At the time of writing, the product's support page - perhaps unsurprisingly thanks to a lack of prior contact with Denev - makes no mention of the alleged vulnerability and the only security related information attached to the device comes via a FAQ which merely states which wireless security standards the product supports.

Denev says the vulnerability lies in the ZynOS firmware used by the modem/wireless router. The popularity of ZynOS means other routers manufactured by D-Link, as well as devices from TP-Link Technologies and ZTE, may also be at risk.

The flaw apparently allows an attacker to access the device's web interface without the need for authentication.

If an administration panel is exposed to the internet - and we strongly recommend that you don't do this! - then outsiders may be able to access and reconfigure your device's DNS setting from afar.

Messing with your DNS settings is a simple but effective way for cybercrooks to direct you to imposter sites, replace adverts on legitimate sites, and even to block or redirect network traffic to keep you away from things like security updates.

This isn't the first time for either D-Link or ZynOS.

In March 2014 Team Cymru, an internet security research organisation, discovered a network containing more than 300,000 compromised routers.

Prior to that, another D-Link security hole was found - "Joel's Backdoor", which provided easy backdoor access to the administration interface on a number of the company's routers.

But of course it's not only D-Link routers which have had their issues - in January 2014 we reported how Sercomm products, which include routers under the LinkSys and Netgear brands, had their own issues surrounding unauthorised admin access.

Chipotle Apologises for Offensive Tweets, Says Account Was Hacked

Fast-food restaurant chain Chipotle was forced to apologise after its Twitter account was used to post racist, homophobic and anti-government tweets on Sunday morning.

The attack, which occurred just after 1am ET, saw the the company's profile picture changed from its usual pepper logo to a swastika. The profile description was also altered to read:

The official Twitter account of @TUGFeds and @TheCeltic666

Both of those accounts have subsequently been suspended by Twitter.

After regaining control of its errant @ChipotleTweets account, the company said sorry to its followers:

We apologize for the very offensive messages sent out from our account earlier tonight. We were unfortunately hijacked temporarily. -Joe

Screenshots captured by Time before the account was reclaimed show some of the offensive tweets, which include anti-establishment messages such as:

F*CK THE GOVERNMENT AND FBI, UR ALL FRAUDS THAT LINE UR POCKETS HAHAAAAH LOSERS, F*CK YOU ALL

In a continuation of the political theme, the attacker also suggested Chipotle was "in full support of the Nazi party" and directed a racial slur at President Obama.

In an official statement, Chipotle's communications director Chris Arnold said:

Our Twitter account was hijacked overnight for about two hours during which a series of offensive tweets was posted to the account.

We apologise for the nature of the posts that were made during that time, and we are now conducting an investigation to try to determine what happened and who might have been involved.

While the motive for the hack is unclear, it is possible that the attackers were acting out of a sense of irony after Chipotle itself seemingly orchestrated a fake Twitter account hack in 2013 - as part of a 20th anniversary publicity campaign.

A series of tweets from the company at first appeared to be random and nonsensical until it later became clear that they contained a list of ingredients for its guacamole recipe. Speaking at the time, Arnold told Mashable that:

We thought that people would pay attention, that it would cut through people's attention and make them talk, and it did that.

It was definitely thought out: We didn't want it to be harmful or hateful or controversial.

The Mexican food chain isn't the first Twitter account to be hacked this

year - in January US pop star Taylor Swift had her account taken over for a short while as an attacker pushed out tweets promoting two other Twitter accounts that were themselves quickly suspended.

As John Zorabedian noted at the time, the best way to protect your own social media accounts from befalling a similar fate is to employ two-factor authentication where available.

Doing so adds an additional layer of security, requiring a would-be attacker to not only circumnavigate your password but also an additional identifying factor, such as a code sent to your phone via SMS.

And, of course, it's really important to make sure you use strong, unique passwords for every single one of your online accounts. If you're not sure what makes a password "strong", then watch our video on how to pick a proper password.

40,000 UnProtected MongoDB Databases Found on the Internet

Nearly 40,000 organisations running MongoDB, a NoSQL high performance and cross-platform document-oriented database, are found to be unprotected and vulnerable to hackers.

Three students from University of Saarland in Germany at the Centre for IT Security Kai Greshake, Eric Petryka and Jens Heyens discovered that MongoDB databases running at TCP port 27017 as a service on several thousands of commercial web servers are easily accessible on the Internet.

MongoDB is an open-source database used by companies of all sizes, across all industries for a wide variety of applications. MongoDB is built for scalability, performance and high availability, scaling from single server deployments to large, complex multi-site architectures. By leveraging in-memory computing, MongoDB provides high performance for both reads and writes.

The German researchers said that they were able to get "read and write access" to the unsecured MongoDB databases without using any special hacking tools. They found 39,890 MongoDB databases openly available on the Internet, including one belongs to an unnamed French telecommunications company containing 8 Million customer s phone numbers and addresses.

"Anybody could retrieve and even alter several million items of customer data, including names, addresses, emails and credit card numbers," the university in Saarbruecken on the Franco-German border said in a statement.

Exploiting the loophole is incredibly easy, as an attacker only needs to run a port scan for TCP port 27017 on the victim s machine and finding all possible vulnerable servers on the Internet could be achieved within four hours by scanning the Internet using fastest TCP Port Scanner called, "masscan".

However, Shodan Search Engine makes the task even easier as it helps hackers to identify accessible MongoDB databases easily. Shodan has a database containing IP addresses with a list of services running and an

easy-to-use filter mask.

The German researchers reported the issue to MongoDB as well as the French Data Protection Authority (CNIL) and the Federal Office for Information Security so that the affected database owners could be notified of the loophole.

MongoDB responded to the issue, saying "MongoDB takes security very seriously." Those who are affected by the issue should use latest installer for MongoDB which limits network access to localhost by default and also refer MongoDB Security Manual.

The Pirate Bay Is Down Again

The saga of The Pirate Bay is far from over. TorrentFreak reported just minutes ago that the popular torrent website has gone offline exactly two weeks after it returned from its extended hiatus. It could be a glitch or a server issue, but based on recent events, it seems just as likely that the site might be back in hot water.

The site still attempts to load after you input the URL, but an "Error 502" message appears in place of the familiar homepage. As TorrentFreak notes, the CloudFlare error indicates that The Pirate Bay's servers are offline.

This is even more worrisome now that other major torrent sites are seeing similar disruptions. Just days ago Kickass Torrents went down and had to move domains.

File Hosting Service RapidShare Shutting Down

Remember RapidShare? Once one of the world's most popular and first ever one-click online file hosting and cloud storage website on the Internet. The company has announced that it will shut down its business at the end of next month.

RapidShare file hosting service announced its shut down Tuesday through a notice on its official website, saying that it will stop active service on March 31, 2015. All user accounts on the website will no longer be available after this date, and all files will be deleted automatically.

"We strongly recommend all customers to secure their data. After March 31st, 2015 all accounts will no longer be accessible and will be deleted automatically," the notice on RapidShare official website reads.

Just two days back, the most popular Torrent website KickAss Torrents banned by the .so registry (Somalian registry), forcing the site's operators to switch to another domain. Now, suddenly the oldest and popular file hosting service is closing up its shop.

RapidShare, founded in May 2002, was widely used to share copyrighted content directly. In 2009, the site claimed to have 10 petabytes of files uploaded to its servers, and in 2010, it was said to have hundreds of

millions of visitors per month, making it among the world's 50 most popular websites.

The reason behind the sudden shutdown decision is still unclear, however, the legal troubles related to copyright infringement have plagued the company for years.

RapidShare has often been faced several lawsuits just like all other notorious file hosting services including The Pirate Bay, Megaupload and Isohunt, which all have been hit with legal issues for facilitating copyright infringement.

While RapidShare worked to cooperate with the entertainment industry and even tried to rebrand itself as a personal cloud storage service in recent years by introducing a number of measures to discourage infringement. But at the end, its user base fell dramatically. It's likely the site simply isn't as profitable as it once was.

The reason behind the closure could also be the increasing competition with the other cloud storage services. We know that RapidShare cloud file hosting servers provides unlimited upload and download sizes, but the service does make you wait to download files if you are not its premium user.

Comparatively, RapidShare charges roughly \$680 per year for 300GB of space, while Dropbox charges just \$99 a year for 1TB.

MegaUpload, one of the largest file sharing websites on the Internet, was shut down in 2012 by federal prosecutors in Virginia, and the site's founder Kim Dotcom and three others were arrested by the police in New Zealand at the request of US authorities, conspiring to commit copyright infringement.

The same happened in the case of The Pirate Bay—a widely popular torrent download website predominantly used to share copyrighted material free of charge, when TPB went dark from the Internet following a raid in Sweden.

The raid was in response to a complaint from Swedish anti-piracy group Rights Alliance. The police raided The Pirate Bay's server room in Stockholm and seized several servers and other equipment. However, the infamous torrent download website The Pirate Bay (TPB) made a defiant return and finally came back online last weekend.

Safer Internet Day 2015

Since 2004, Net activists, educators, parents, technology companies and geeks around the globe have been gathering each February to celebrate Safer Internet Day. Their goal: To promote responsible behavior online and in the mobile world, especially among kids.

This year's US commemoration, organized by ConnectSafely.org, will take place Tuesday afternoon at Facebook's Palo Alto headquarters.

California State Attorney General Kamala Harris will deliver the keynote address, following an introduction by Facebook Chief Operating Officer Sheryl Sandberg. Harris will be followed by a panel discussion moderated by Yahoo Tech's own Dan Tynan, which will focus on finding solutions to

the problem of online bullying, trolls, and social cruelty.

Other panels will include a discussion of how to use technology to effect social change, and a conversation with industry leaders from Google, Twitter, and Instagram moderated by Stephen Balkam, founder and CEO of the Family Online Safety Institute.

Safer Internet Day, which began in Europe before spreading to the US, will be celebrated in more than 100 countries worldwide.

'Revenge Porn' Law Passed in England and Wales

A new law banning "revenge porn" - sexually explicit images shared online by a former partner without their ex's consent - was passed in England and Wales Thursday.

The law means that people caught sharing such images on social networking sites like Facebook and Twitter or via SMS and email could face up to two years in prison.

England and Wales join jurisdictions including Japan and the US state of California in banning such images.

The move was welcomed by women who featured in "revenge porn" shared by their former partners, as well as women's groups.

Hannah Thompson, 22, discovered that her ex-boyfriend had been publishing explicit photos of her on his blog, tagged with offensive captions.

She campaigned for a change in the law and her case was quoted during debate on the issue in the House of Commons.

Thompson called the law change, plus guidelines for police on prosecuting cases and a new support helpline, "huge steps forward".

"It's a clear sign that they (the victims) are not to blame, they are not in the wrong and there is support out there for them," she said.

Folami Prehaye's ex-partner shared explicit pictures of her on Facebook after she left him last year.

She has now set up a website, Victims of Internet Crime (VOIC), to support others in the same situation.

While welcoming the changes, she said that more needed to be done to alter attitudes.

"A law change is a law change but it doesn't necessarily deter people," she told AFP.

"When my ex-partner did that, I know he did it out of anger. I had pictures of him but I just deleted them - that's rational."

The new law applies to "photographs or films which show people engaged in sexual activity or depicted in a sexual way or with their genitals exposed," the Ministry of Justice said.

Some "revenge porn" offences were already illegal under existing legislation banning harassment and malicious communications.

But the new law toughens up the legal situation following technological advances which campaigners say have made the problem more common in recent years.

Campaign group End Violence Against Women welcomed the ban, saying "revenge porn" was "used by abusive partners and ex-partners as a way of threatening, controlling and hurting women."

"So-called 'revenge pornography' is also extremely harmful because the person uploading or sharing does so without the victim's consent and often with the intent to harm and humiliate," acting director Sarah Green added.

"It is abusive behaviour and should be treated the same way as offline abuse."

While the law does not force social media sites to remove "revenge porn", the Ministry of Justice said it would "send out a clear message and make it easier for social media providers to act."

How One Man Could Have Deleted Any Photo Album He Could See on Facebook

Facebook is probably the biggest database of photographs ever compiled.

We upload around 350 million photos to the world's most popular social network every day. Facebook users aren't quite as busy sharing photos as the kids who use Snapchat or WhatsApp but they're not far off, and they've been doing it a lot longer.

In a beautiful and terrifying illustration of the vast asymmetries that the internet can create, security researcher Laxman Muthiyah has revealed how he discovered he had the power to delete billions of images. If he was allowed to see it, he was allowed to delete it.

Thankfully for Facebook's 1.3 billion users Laxman's moral compass was in fine working order that day. He reported the bug to Facebook as soon as he found it, netting himself a cool \$12,500 USD bug bounty in return.

Facebook's response was swift - to its great credit the bug was fixed across its vast network within 2 hours.

In Laxman's own words:

OMG :D the album got deleted! So i got the key to delete all of your Facebook photos :P lol :D?Immediately reported this bug to Facebook security team. They were too fast in identifying this issue and there was a fix in place in less than 2 hours from the acknowledgement of the report.

And let's be absolutely clear, Laxman had options.

The bug he discovered is a weapon. It wouldn't have killed anyone but it could have caused misery to to millions.

Laxman could probably have sold that bug to somebody other than Facebook and earned a great deal more money than he got for doing the Right Thing.

Or he could have milked it; kept his discovery under wraps (giving somebody less upstanding a chance to find it), engaged a PR firm and given it a fancy name.

And of course he had the chance to make himself The Man That Wrecked Facebook if he wanted to take it. Do you think LizardSquad would have blinked before inflicting misery for the sake of self-aggrandisement?

Kudos Laxman.

You might think that pulling off something like this requires genius and technology on an equally epic scale.

Not a bit of it.

In theory you could do it with a few lines of code and a phone or a Raspberry Pi. Hell, the code would probably run on a digital watch.

In practice Facebook probably operates rate limiting or other countermeasures that would prevent a single device from doing too much harm - and even if it doesn't, the social network is so large an attacker would probably struggle to delete albums as fast as people on Facebook create new ones.

But that's just a question of horsepower, and horsepower is easy on the internet - there are kids running botnets of 60,000 computers.

Laxman discovered the bug whilst poking about in Facebook's Graph API (Application Program Interface).

The Graph API is the official Facebook interface for websites, apps and other computer programs that want to integrate with Facebook.

Unlike the glossy, graphical, point-and-click interface that we humans use, it's a terse, code interface that's driven by HTTP requests rather than taps, typing or mouse clicks.

It allows computer programs to do the same things that humans can do with Facebook and much more besides.

Just like the human interface, users of the API are not supposed to be able to edit or delete things that belong to somebody else.

What Laxman discovered was a bug that allowed him to do just that if he used a Facebook for Android access token to authenticate himself.

So long as he had the photo album id and permission to view the album he could delete it. The anti-Facebook super-weapon was no more than a four line HTTP request:

```
DELETE /<victim's album id> HTTP/1.1
```

```
Host : graph.facebook.com
```

```
Content-Length: 245
```

```
access_token=<attacker's Facebook for Android token>
```

Facebook album IDs are numeric, which means that guessing them is easy - you start with 1 and just keep going up.

So wrap that 4 line request in a loop and increment the ID from one to a trillion and you've got yourself a micro-David to take on Facebook's photographic mega-Goliath.

Update 2015-02-12

Facebook got in touch, keen to explain that this bug only applies to photo albums that the attacker has permission to view which, to all practical purposes, means photo albums that are public.

Your Cover Photos and Profile Pictures albums are public by default, for instance.

Taking out those albums alone, never mind any other public albums, would still amount to a hugely damaging attack but in light of this information we've changed the original headline and two sentences in the article to better reflect the nature of the bug.

Facebook's spokesperson said:

We received a report about an issue with our Graph API and quickly fixed it within two hours of verifying the claims. To be clear, triggering this issue would have required knowledge of the ID of the target photo album, as well as permission to view the album based on the album's privacy settings. We'd like to thank the researcher who reported the issue to us through our bug bounty program.

Microsoft Might Make You Pay Every Year To Use Windows in the Future

Microsoft might make you pay every year to use Windows in the future. Microsoft might be ready to offer Windows 10 as a free download to certain customers later this year, but the company still has plans to make plenty of money off of its most important product. In addition to enterprise customers that'll have to pay for the upgrade to Windows 10, the company might also have a different kind of Windows product in mind, one that will have a subscription business model like Office 365.

FROM EARLIER: Windows 10 won't be as free as you might have hoped. The term Windows 365 has been listed in various leaks detailing some of Microsoft's plans for the future, with people speculating that the company is interested in bringing the Office 365 model to Windows in the future.

It looks like the marketing name is definitely genuine, Neowin reports, as the company has applied for a Windows 365 trademark.

However, it's not clear what the company plans to do with Windows 365 in the future, and the publication says Microsoft might be simply taking defensive action for the time being, looking to protect this particular trademark for the future.

New York Could Become First City To Accept Bitcoin

New York City Councilman Mark Levine is expected to unveil a proposal on Thursday that will allow the city to accept bitcoin as payment for fines.

The bill would allow the municipality to accept the cryptocurrency for things like parking tickets and court fees, but could also include an added charge for bitcoin payments.

The bill is still in its infancy and will need to be reviewed by the city's officials before becoming a law; if passed, it would be hailed as a huge step toward mainstream adoption for bitcoin.

Late last year, New York began working to find ways to make parking tickets easier to pay, which is where the concept of bitcoin payments was born.

City finance officials were considering the use of a smartphone app that would allow ticket holders to pay using Apple Pay, PayPal or bitcoin.

Since then, lawmakers have been working out the details of creating such an app and debating the merits of incorporating bitcoin into the system.

New York is not the first state to explore the possibility of using cryptocurrency for fees and fines.

In 2014, Pittsburgh also examined the benefits of allowing its residents to make bitcoin payments, but ultimately decided against it.

The city's officials, who were working to avoid bankruptcy at the time, said the currency was too volatile and new to be considered as a viable option. Instead, they chose to focus on more popular forms of payment like credit and debit.

Facebook Is Telling Native Americans Their Names Are Fake

In October, Facebook apologised to the drag queens, drag kings, and others in the LGBT (lesbian/gay/bisexual/transgender) community, some of which it had recently locked out of their accounts because their names weren't "real."

Facebook owned up to a policy that was essentially clueless about the importance of using pseudonyms online to protect people from harassment and violence.

Changes are in the works, Facebook promised at the time.

But missing from that apology and mea culpa: an apology to all the Native Americans who are still getting locked out when they use their real names.

As reported by Colorlines, Facebook is telling them that their user names are fake.

Facebook is actually now calling its "real name" policy the "authentic" name policy, but the gentler name doesn't make any difference for Native Americans.

That's because Facebook's baked an anti-Native name slant into its policy. For example, the company explicitly prohibits using "words, phrases or nicknames in place of a middle name".

That means that a Native named In Between The Watchers, for example, is in violation of the policy.

Natives claim that the social media behemoth is forcing them to jump through hoops to prove they're real - including requesting documents such as credit cards or taxpayer IDs to support their claims.

One such is Dana Lone Hill: one of the Lakota people who writes that she was shut out when she used her father's and mother's last names (respectively, Lone Elk and Lone Hill).

Lone Hill did what Facebook's automatic "Please Change Your Name" message requested, sending in three forms of ID: her library card, one with a picture, and a piece of mail.

Be patient, Facebook's bot responded: we'll investigate and get back to you.

She was able to log back in, briefly, the day after it was suspended, but then she got locked out again.

Lone Hill writes that she initially felt singled out, but a bit of exploration revealed she wasn't the only one:

I had a little bit of paranoia at first regarding issues I had been posting about until I realized I wasn't the only Native American this happened to. One friend was forced to change his name from his Cherokee alphabet to English. Another was forced to include her full name, and a few were forced to either smash the two word last names together or omit one of the two words in the last name. Oglala Lakota Lance Brown Eyes was [booted] from Facebook and when he turned in his proof of identification they changed his name to Lance Brown. After contacting the Better Business Bureau and threatening Facebook with a class action lawsuit, they sent him an apology and let him use his given name again.

Profiles get reported as "fake" when individuals flag them.

It's happened twice to Shane Creepingbear, the most recent time being in October.

Creepingbear is a member of the Kiowa Tribe of Oklahoma, and that's really, truly his last name. But Facebook didn't buy it, he told The Washington Post.

I started going through the remediation process to prove that I was a real person. They kept asking me to put in my real name. And they said this doesn't meet Facebook's standards.

I had to send in a photo of my state ID and I had done that before and that was very frustrating for them to demand it again. It just felt really marginalizing.

Natives have a few options: Choosing a Facebook-friendly version of their real names is one option.

True, it will probably keep people from reporting an account as fake, but many would see it as demeaning and prejudicial. As the Washington Post said:

For many Native Americans, being forced to "prove" their identities is

more than an inconvenience; it is a form of silencing.

If somebody does report a Native name as being inauthentic, it's up to Facebook employees to determine the issue - a subjective process that's not guaranteed to be resolved in the user's favour.

Lone Hill told the Post that it sounds like a matter of ignorance on Facebook's part, just like how it was oblivious about its real name policy's implications for the LGBT community:

I just think they have to maybe have more training on what our full names encompass. ... We hang on to these names. A lot of [Native Americans] went with Christian last names and lost their names, so we carry these names proudly.

I asked Facebook if policy changes were in the works.

A spokesperson noted that over the past six months, Facebook's added a new option for verifying names: one that allows someone with an "authentic" name that isn't necessarily a "legal" name to provide one ID with the legal name and a few more pieces of documentation for the name he or she goes by.

That's option 3 on its Help Center page.

The spokesperson also sent this statement:

We are committed to ensuring that all members of the Facebook community can use the authentic names that they use in real life. Having people use their authentic names makes them more accountable, and also helps us root out accounts created for malicious purposes, like harassment, fraud, impersonation and hate speech. Over the last several months, we've made some significant improvements in the implementation of this standard, including enhancing the overall experience and expanding the options available for verifying an authentic name. We have more work to do, and our teams will continue to prioritize these improvements so everyone can be their authentic self on Facebook.

The company responded slowly to the LGBT community, but eventually, it did respond. Changes are still in the works, as it said.

Based on its past response on this issue, I'm hoping, and am pretty sure, that it's again going to do the right thing.

Facebook Now Lets You Choose Who Controls Your Account After You Die

Facebook is putting its users in control of what happens to their accounts after they die. Starting today, users in the US will be able to choose to have their accounts deleted after death or grant another person on Facebook permission to manage an account on their behalf. Facebook calls this person an account's legacy contact, and users will be able to choose that person through the website's or app's security page.

If you chose to set up a legacy contact, that person will be able to change your profile photo, accept friend requests, and pin announcements on your account's timeline after Facebook receives notice of your death. A legacy contact won't be able to post as the account that they're

controlling, nor will they be able to view that person's private messages. Facebook will also provide an option to let legacy contacts download a file containing an account's photos, posts, and other information.

Before today, Facebook provided a process to freeze accounts after death, but there was no way to set them up to be managed by someone else or automatically deleted. Facebook said last year that it was working on better ways to handle accounts after death. At the time, it started respecting users' existing privacy settings and allowing Look Back compilation videos to be generated. Now, about a year later, it's actually giving its users control. Setting up legacy choices is optional, and Facebook says that they'll eventually roll out to other countries.

==~==~==

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.